

AN ASYMMETRIC SYSTEM AND METHOD FOR TAMPER-PROOF STORAGE OF AN AUDIT TRAIL FOR A DATABASE

Abstract

An asymmetric key based method and system is provided for a tamper-proof storage of one or more records of an audit trail for a database. The asymmetric key based key exchange mechanism is employed to arrive at a common key, which is then used to obtain the authentication and the validation tokens. The method creates one or more authentication token values, and generates one or more validation token values from the authentication token values through a combination of a hashing process and an encryption process. Once the validation token values are created, they are further integrated into the records in the database. When an authorized person such as an auditor who needs to check the integrity of the records, he can detect a tampering of the records by comparing a validation token value newly computed by him independently with the validation token value integrated in the record.